WHAT IS CLAIMED IS:

1. A method for validating the integrity of a target data file loaded on a computing device, the method comprising:

providing a portable cryptographic device having a software verification key, the portable cryptographic device being coupled to a computing device;

identifying a target data file for validation on the computing device; and

generating a software verification value for the target data file using the software verification key.

2. The method of Claim 1 further comprising storing the software verification value on the portable cryptographic device.

3. The method of Claim 1 further comprising storing the software verification value on the computing device.

4. The method of Claim 1 further comprising:

receiving a user identification; and

validating the user identification against a secret user information, wherein the secret user information is provided on the portable cryptographic device.

5. The method of Claim 4, wherein the user identification comprises a password.

6. The method of Claim 4, wherein the user identification comprises a personal identification number.

7. The method of Claim 4, wherein the user identification comprises a bio-metric data.

8. The method of Claim 1 further comprising:

requesting a previously generated software verification value; and

comparing the software verification value with the previously generated software verification value.

9. The method of Claim 8, wherein comparing the software verification value is performed in response to a startup of the target data file.

10. The method of Claim 1, wherein the portable cryptographic device is a smart card.

11. The method of Claim 1, wherein the portable cryptographic device is a USB connected module.

12. The method of Claim 1, wherein generating the software verification value comprises a secure hashing calculation.

13. The method of Claim 1, wherein generating the software verification value comprises an encryption calculation.

14. The method of Claim 1, wherein generating the software verification value comprises a message authentication calculation.

15. The method of Claim 1, wherein generating the software verification value comprises a digital signature.

16. The method of Claim 1, wherein the target data file comprises an operating system.

17. The method of Claim 1, wherein the target data file comprises an application program.

18. The method of Claim 1, wherein the software verification value is generated in response to detecting an install of the data file.

19. The method of Claim 1, wherein the software verification value is generated in response to detecting a closing of the data file.

20. The method of Claim 1, wherein the software verification value is generated in response to detecting a shutdown of the computing device.

21. The method of Claim 1, wherein the generating the software verification value is performed by logic on the portable cryptographic device.

22. The method of Claim 1, wherein the generating the software verification value is performed by logic executing on the portable cryptographic device.

23. The method of Claim 1, wherein the generating the software verification value is performed by logic executing on the computing device.

24. An apparatus for validating integrity of a data file, the apparatus comprising:

a software verification key being provided on a portable cryptographic device; and

a security logic coupled to the software verification key, the security logic operable to receive as input a target data file loaded on a computing device, the security logic operable to generate a software verification value for the target data file using the software verification key.

25. The apparatus of Claim 24, wherein the security logic executes on the portable cryptographic device.

26. The apparatus of Claim 24, wherein the security logic executes on the computing device.

27. The apparatus of Claim 24, wherein the portable cryptographic device is coupled to the computing device.

28. The apparatus of Claim 24, wherein the security logic is further operable to store the software verification value on the computing device.

29. The apparatus of Claim 28, wherein the software verification value is a protected software verification value.

30. The apparatus of Claim 24, wherein the security logic is further operable to receive as input a user identification and validate the user identification against a secret user information, the secret user information being provided on the portable cryptographic device.

31. The apparatus of Claim 24, wherein the security logic is further operable to request a previously generated software verification value and compare the software verification value against the previously generated software verification value.

32. A computer-readable storage medium having stored thereon computer instructions that, when executed by a computing device, cause the computing device to:

detect a status change in a data file, the data file being loaded on a computing device;

request a software verification key, the software verification key being provided on a portable cryptographic device, the portable cryptographic device being coupled to the computing device; and

request a software verification value calculation for the data file, the software verification value calculation comprises a mathematical manipulation of the data file using the software verification key.

33. The computer-readable storage medium of Claim 32, wherein the software verification value calculation is performed on the computing device.

34. The computer-readable storage medium of Claim 32, wherein the software verification value calculation is performed on the portable cryptographic device.

35. The computer-readable storage medium of Claim 32, wherein the status change comprises an install of the data file.

36. The computer-readable storage medium of Claim 32, wherein the status change comprises a closing of the data file.

37. The computer-readable storage medium of Claim 32, wherein the status change comprises a shutdown of the computing device.

38. The computer-readable storage medium of Claim 32, wherein the computer instructions that detect a status change in a data file further comprise computer instructions that, when executed by a computing device, cause the computing device to:

receive a user identification; and

validate the user identification against a secret user information, the secret user information being provided on the portable cryptographic device.

39. The computer-readable storage medium of Claim 32, wherein the computer instructions that detect a status change in a data file further comprise computer instructions that, when executed by a computing device, cause the computing device to:

request a previously generated software verification value for the data file; and

compare the software verification value with the previously generated software verification value.

40. The computer-readable storage medium of Claim 39, wherein the compare of the software verification value is performed in response to detecting a startup of the data file.